

OFFICE OF THE COMPTROLLER

Quality Assurance Bureau

Internal Control Guide

9/13/2007

OFFICE OF THE COMPTROLLER

Internal Control Guide

1 Ashburton Place, 9th Floor
Boston, Massachusetts 02108
www.mass.gov/osc

<u>MEMORANDUM</u>	<u>3</u>
<u>INTRODUCTION</u>	
<u>ACKNOWLEDGEMENTS.....</u>	<u>4</u>
<u>CHAPTER ONE: INTERNAL CONTROL PLAN FRAMEWORK</u>	
<u>TONE AT THE TOP</u>	<u>6</u>
<u>MANAGEMENT PHILOSOPHY & OPERATING STYLE.....</u>	<u>7</u>
<u>ETHICS</u>	<u>7</u>
<u>ACCOUNTABILITY.....</u>	<u>7</u>
<u>MISSION STATEMENT</u>	<u>8</u>
<u>GOALS</u>	<u>8</u>
<u>OBJECTIVES</u>	<u>8</u>
<u>ORGANIZATIONAL STRUCTURE</u>	<u>9</u>
<u>COMPETENCE.....</u>	<u>9</u>
<u>EFFECTIVENESS & EFFICIENCY.....</u>	<u>9</u>
<u>EVENT IDENTIFICATION.....</u>	<u>9</u>
<u>RISK ASSESSMENT</u>	<u>10</u>
<u>RISK RESPONSE.....</u>	<u>10</u>
<u>CONTROLS</u>	<u>10</u>
<u>POLICIES AND PROCEDURES</u>	<u>10</u>
<u>SECURITY</u>	<u>11</u>
<u>SEGREGATION OF DUTIES.....</u>	<u>12</u>
<u>INFORMATION.....</u>	<u>12</u>
<u>COMMUNICATION.....</u>	<u>13</u>
<u>MONITORING</u>	<u>14</u>
<u>AUTHORIZATION.....</u>	<u>15</u>
<u>PERIODIC COMPARISON/RECONCILIATION.....</u>	<u>15</u>
<u>CONTINUOUS SUPERVISION</u>	<u>15</u>
<u>RECORDING TRANSACTIONS</u>	<u>15</u>
<u>ACCESS TO RESOURCES.....</u>	<u>15</u>
<u>DOCUMENTATION.....</u>	<u>16</u>
<u>CHAPTER TWO: EVALUATING THE INTERNAL CONTROL PLAN</u>	
<u>EVALUATION POINTS.....</u>	<u>17</u>
<u>CHAPTER THREE: INTERNAL CONTROL PLAN WORKBOOK</u>	
<u>GETTING STARTED (QUESTIONS YOU MUST ASK).....</u>	<u>19</u>
<u>YOUR WORKBOOK (LINKING INTERNAL CONTROLS TO RISKS).....</u>	<u>21</u>

CHAPTER FOUR: ANNUAL REPORTING

<u>INTERNAL CONTROL QUESTIONNAIRE.....</u>	<u>23</u>
---	------------------

APPENDIX 1: REGULATIONS AND GUIDANCE

<u>CHAPTER 647 OF THE ACTS OF 1989</u>	<u>25</u>
<u>COSO</u>	<u>25</u>
<u>YELLOW BOOK.....</u>	<u>27</u>
<u>SARBANES-OXLEY (SOX).....</u>	<u>28</u>
<u>OMB CIRCULAR A-123</u>	<u>28</u>
<u>OMB CIRCULAR A-133</u>	<u>29</u>
<u>SAS NO. 112</u>	<u>29</u>
<u>AUDIT COMMITTEE</u>	<u>29</u>
<u>INTERNAL AUDIT.....</u>	<u>30</u>

APPENDIX 2: WORKS CITED.....



MARTIN J. BENISON
COMPTROLLER

Commonwealth of Massachusetts
Office of the Comptroller
One Ashburton Place, Room 901
Boston, Massachusetts 02108

Phone (617) 727-5000
Fax (617) 727-2163
<http://www.mass.gov/osc>

Memorandum

To: Legislative Leadership, Judicial Branch Administrators, Elected Officials, Secretariats, and Department Heads, Chief Fiscal Officers, MMARS Liaisons, Internal Control Officers and Payroll Directors

From: Martin J. Benison, Comptroller

Date: 09/13/2007

Re: **Revised – Commonwealth Internal Control Guide**

I am pleased to issue this revised Internal Control Guide that streamlines the content of the existing manuals and incorporates the principles of Enterprise Risk Management (ERM) that tie risk to strategic planning. These principles reflect the concepts of broad-based objective setting, event identification, and risk response. This new guide replaces both the *Internal Control Guide for Managers, Volume I*, and *Internal Control Guide for Departments, Volume II*. This guide is based on the standards of the 1994 Committee of Sponsoring Organizations of the Treadway Commission (COSO) Report, as well as its framework for Enterprise Risk Management (ERM) which was released in 2004.

The new format is designed to assist departments in preparing internal controls and Internal Control Plans (ICPs), acknowledging that each department has unique risks. Please remember that an effective ICP is a high level, department-wide summarization of risks and controls for all of its business processes and is supported by lower level detail. Because internal control is a basic responsibility of all managers, we recommend that Internal Control Officers distribute this guide, along with your current Internal Control Plan, to all of your department's managers. Departments must update the ICP as often as changes occur in management, level of risk, program scope, etc., but at least annually.

Questions or comments should be addressed to the Quality Assurance Bureau at 617-973-2450.

To register for training workshops, please refer to the [CTR Training and Meeting Schedule](#).

Introduction

Beginning with Watergate in the early 1970s, political and corporate corruption introduced the need for a method to monitor organizational activities. The Savings and Loan crisis soon followed these events. During the 1980s, numerous instances of inappropriate activities caused massive savings and loan association failures in the United States. By the end of the crisis, over 1,000 regularly audited savings and loan institutions failed, at a cost of \$150 billion. Congress began investigating the crisis, culminating in the introduction of legislation intended to provide oversight to the audit profession. In response, the major audit associations united to sponsor the Treadway Commission. In 1987, the Treadway Commission issued its initial report, recommending that the organizations sponsoring the Commission work together to develop integrated guidance on internal control. The sponsoring groups accepted the recommendation, forming the Committee of Sponsoring Organizations (COSO). A Congressional majority determined that these actions by audit organizations meant that the legislation was unnecessary.

In the Commonwealth of Massachusetts, the State Auditor introduced legislation requiring the development and implementation of internal controls for Commonwealth agencies. As a result, Massachusetts became one of the first states to enact internal control legislation. This Legislation, known as Chapter 647 of the Acts of 1989, *An Act Relative to Improving the Internal Controls within State Agencies*, directed the Office of the Comptroller (CTR) to develop internal control guidelines for state agencies. This document is the seventh edition of the Internal Control Guide, first published by the Office of the Comptroller in 1987.

After COSO issued its report in 1992, various accounting organizations and the U.S. General Accounting Office (GAO) also began developing internal control guidance. By 2002, a wave of separate, but related, accounting scandals at companies like Enron and WorldCom became known to the public. This further evidence of inappropriate conduct renewed congressional interest in mandating requirements for stricter internal controls. These controls, based on COSO and on the guidance developed by accounting organizations, culminated in the passage of the Sarbanes-Oxley Act.

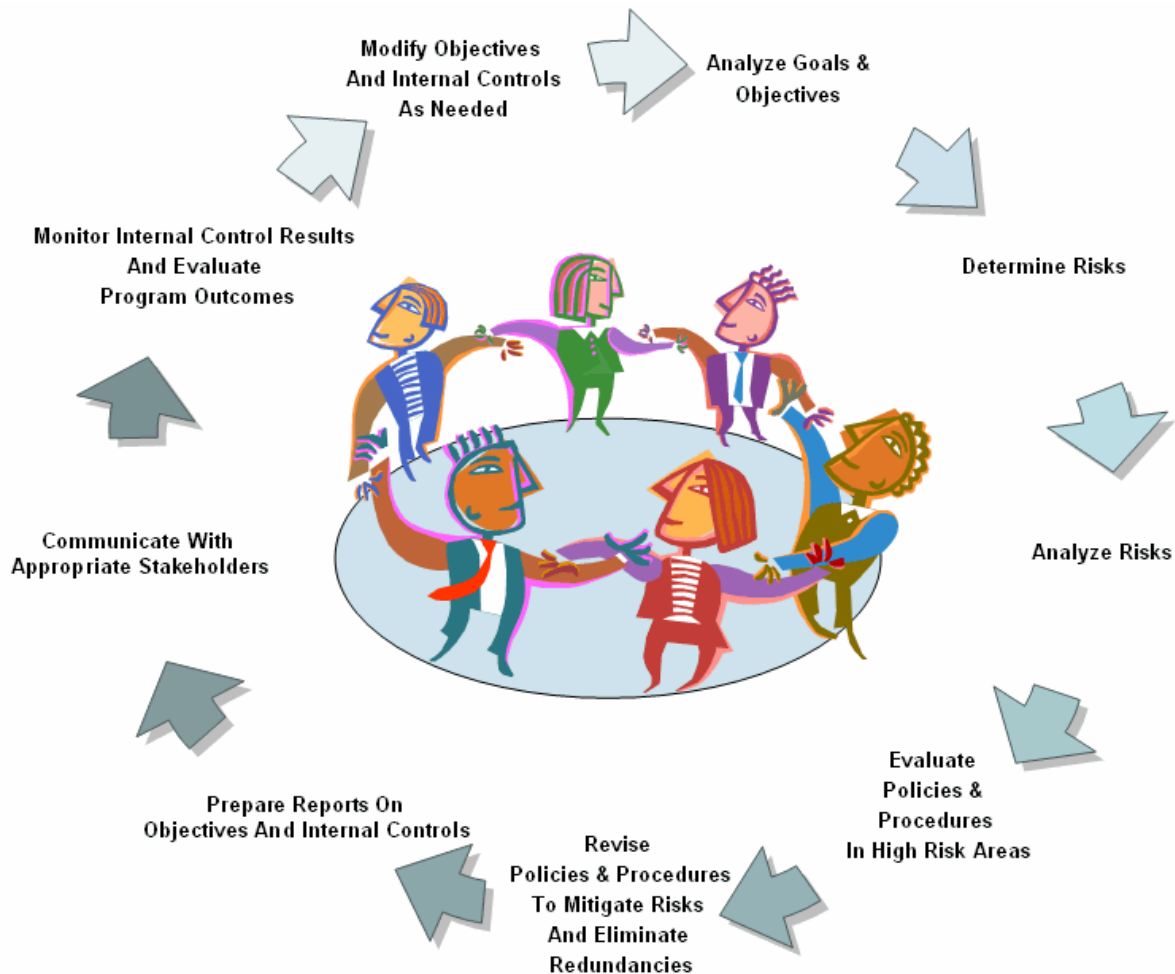
Internal control standards continue to evolve as audit organizations and government agencies use their experiences to refine and reshape the concept of acceptable internal control. Appendix 1 contains additional information on the regulations and guidance discussed above.

Acknowledgements

The Office of the Comptroller (CTR) acknowledges the generous assistance of everyone who made this guide a reality. The Office of the State Auditor (OSA) and staff within the CTR deserve special recognition.

Internal Control Plan Framework

Internal Control Plan and Risk Assessment Cycle



An organization is a living entity which changes over time. As a result, the organization's mission, goals and objectives must be regularly evaluated and periodically revised. Thus, internal control is an ongoing process

known as the Internal Control Cycle. After an organization analyzes its goals and objectives to determine its risks, management must analyze these risks and evaluate the policies and procedures in the identified high-risk areas. Part of the management process includes monitoring the progress made toward meeting goals and objectives. Monitoring also helps to ensure the effectiveness of the organization's internal controls and the effectiveness of the policies and procedures. Periodically, policies and procedures should be revised to mitigate risk and eliminate redundancy. They must also be communicated internally and externally, as necessary.

Everyone in an organization has responsibility for internal control.

An internal control plan is a description of how a department expects to meet its various goals and objectives by using policies and procedures to minimize risk. The Commonwealth has defined the internal control plan to be a high-level summary supported by lower level policy and procedures. Each department's internal control plan will be unique; however, it should be based on the same framework – the organization's mission statement, goals and objectives, and components of internal control recommended by COSO. The plan should be reviewed and updated as conditions warrant, but at least annually.

Because the department's policies and procedures provide the detail for the internal control plan, it is important that they be reviewed in conjunction with the plan. It is not uncommon for the detailed policies and procedures to be modified due to changes in personnel, audit or quality assurance recommendations, etc. As these modifications occur, the department's documentation should be updated to reflect them.

As stated in Chapter 647 of the Acts of 1989, the department's Internal Control Officer is responsible for its internal control plan. The designated Internal Control Officer should be a senior manager, equivalent in title or rank to an assistant or deputy to the department head. It should be noted, however, that internal controls are the responsibility of every employee.

This chapter will discuss some concepts related to the Enterprise Risk Management (ERM) components of Internal Environment, Objective Setting, Event Identification, Risk Assessment, Risk Response, Control Activities, Information & Communication and Monitoring. It is important to realize that ERM is not a linear process but rather a multi-directional process in which almost any component can, and will, influence another component.

Tone at the Top

Management's attitude, actions, and values set the tone of an organization, influencing the control consciousness of its people. Internal controls are likely to function well if management believes that those controls are important and communicates that view to employees at all levels. If management views internal controls as unrelated to achieving its objectives, or even worse, as an obstacle, this attitude will also be communicated. Employees are aware of the practices followed by upper management including those that circumvent internal controls. Despite policies to the contrary, employees who note that their managers frequently override controls, will also view internal controls as "red tape" to be "cut through" to get the job done. Management can show a positive attitude toward internal control by such actions as complying with their own policies and procedures, discussing internal controls at management and staff meetings, and rewarding employees for following good internal control practices. Although it is important to establish and implement policies and procedures, it is equally important to follow them.

Management Philosophy & Operating Style

Management's philosophy and operating style affect the way the organization is managed. They determine, for example, whether the organization functions informally with verbal instructions or formally with written policies and procedures. They also define whether the organization is conservative or aggressive in its response to risks. In other words, they define the organization's "risk appetite" or the level of risk that is acceptable to the organization. To be successful, the organization's internal controls must be aligned with management's philosophy.

Ethics

An organization's culture evolves from the values of its members and the culture, in turn, exerts a strong influence on the actions, decisions, and behaviors of all employees.

Massachusetts officials' or employees' conduct is also governed by M.G.L. c. 268A. The [Conflict of Interest Law](http://www.mass.gov/ethics/web268A.htm) (<http://www.mass.gov/ethics/web268A.htm>) regulates the conduct of all state, county and municipal employees and volunteers, whether paid or unpaid, full or part-time, intermittent or temporary. General Law Chapter 268A governs what public officials and employees may do on the job, what they may do after hours, or on the side, and what they may do after they leave public service. See also, [Introduction to the Conflict of Interest Law for the Public Officials and Public Employees](http://www.mass.gov/ethics/public_sector.html). (http://www.mass.gov/ethics/public_sector.html)

Accountability

Public sector managers are responsible for administering the resources entrusted to them to carry out government programs. A major factor in fulfilling this responsibility is ensuring that adequate internal controls exist. Public officials, legislators, and taxpayers are entitled to know whether government agencies are properly handling funds and complying with laws and regulations. They need to know whether government organizations, programs, and services are achieving the purposes for which they were authorized and funded. Officials and employees who manage programs must be accountable to the public. Frequently specified by law, this concept of accountability is intrinsic to the governing process of the Commonwealth of Massachusetts. Internal control is a technique used by managers to help a department achieve these objectives. Internal control is the term we use for the structure, policies, and procedures used to ensure that the department accomplishes its objectives and meets its responsibilities.

An ethical culture requires engaged employees and managers who understand why doing the right thing is important for the organization's long-term viability; and they have the determination to see that in fact the right thing does get done.

What are some of the key attributes needed for an organization to be fully integrity-based?

- Employees feeling a sense of responsibility and accountability for their actions and for the actions of others.
- Employees freely raising issues and concerns without fear of retaliation.
- Managers modeling the behaviors they demand of others.
- Managers communicating the importance of integrity when making difficult decisions.
- Leadership understanding the pressure points that drive unethical behavior.
- Leadership developing processes to identify and remedy these areas where pressure points occur.

These attributes touch other aspects of the organization that go beyond the fundamental abilities of making a profit and maintaining high levels of quality and productivity: how well the organization adapts to change, or encourages employees to be engaged in decision making, how well the organization creates a collective sense of purpose around shared values. It is this broader set of skills and qualities that create the foundation needed to support an ethical culture. These higher-level behaviors are no longer "nice to have." These are the behaviors now demanded by the SEC and the DOJ.

- www.workingvalues.com

Mission Statement

A mission statement clearly identifies an organization's purpose and how it is accomplished. It should be a brief paragraph that is easily understood by the reader, including those outside the organization or field. The mission statement, therefore, should be free of jargon and/or shorthand.

An organization's mission statement may remain current for a number of years. However, it is a good idea to review it periodically – such as part of the annual internal control plan review – to fine-tune or update it.

Goals

A goal is an end result the organization wants to attain. It should be a broad, long-range concept and not limited to what can be accomplished in a single fiscal year. When an organization sets its goals, it is determining its priorities.

Government managers set department goals and priorities based upon legislative mandates established in statutes (enabling legislation), priorities of the Governor and Cabinet Secretaries, and within funding authorization set in annual appropriations.

Objectives

An objective is the action required to achieve the long-range goal. In contrast to a goal, an objective is narrowly focused and easily validated. It should, therefore, be an action that can be accomplished in an identified period of time, such as a fiscal year. A good objective is **SMART**:

Specific – What is the single result to be accomplished?

Measurable – How can it be measured? (Some objectives are more difficult to measure; however, they should have observable results.)

Attainable – Is it realistic given the resources currently available?

Results-focused – Does it make a difference if the objective is accomplished?

Timely – Is the timeline realistic?

Mission Statement

"To provide every resident of Massachusetts with equal opportunity to access information resources that will satisfy individual educational, working, cultural, and leisure-time needs and interests, regardless of an individual's location, social or physical condition, or level of intellectual achievement."

- Board of Library Commissioners

"EEC will lead the way in helping Massachusetts children and families reach their full potential. By providing and coordinating a range of services and assistance, EEC will continuously improve the quality, affordability, and accessibility of early education and care in the Commonwealth.

- Department of Early Education and Care

The mission of the Massachusetts Department of Revenue is to achieve maximum compliance with the tax, child support and municipal finance laws of the Commonwealth. In meeting its mission, the Department is dedicated to enforcing these laws in a fair, impartial and consistent manner by providing professional and courteous service to all its customers.

- Department of Revenue

We promote the independence and well-being of elders and people needing medical and social supportive services by providing advocacy, leadership, and management expertise to maintain a continuum of services responsive to the needs of our constituents, their families, and caregivers.

- Executive Office of Elder Affairs

Goals & Objectives

Goal: To provide guidance to departments seeking to develop / update their internal control plans.

Objective #1: Issue a revised Internal Control Guide by September, 2007.

Objective #2: Develop program to introduce revised Internal Control Guide to departments by October, 2007.

Objective #3: Provide half-day, hands-on workshops in October and November, 2007.

Organizational Structure

The organizational structure provides the decision-making framework of an organization. This structure groups, divides, and coordinates the tasks required to achieve identified goals. To be effective, the structure must make the best use of available resources while maintaining adequate controls to ensure compliance with state finance and other applicable requirements.

Competence

There are two types of competencies – position and personal. Position competencies are the skills needed to perform the required duty, regardless of the incumbent. Personal competencies are the skills, knowledge, expertise, and experience of the individual employee, regardless of whether they are tied to the employee's current position. Employees should have the skills to adequately perform their assigned duties.

Effective human resource policies strengthen an organization's internal controls. These policies should address hiring, training, performance evaluations, responsibilities, appropriate behavior and disciplinary actions. If employees understand that they are responsible and accountable, the control environment is strengthened.

An employee handbook can enhance an agency's control environment. It should include, but not be limited to, departmental policies and procedures, control procedures, employee responsibilities, ethics, description of employee evaluations, job descriptions and possible disciplinary action to take when standards are violated.

Effectiveness & Efficiency

Effectiveness and efficiency are the most fundamental management responsibilities. Effectiveness is judged on the basis of results. We judge success by evaluating the effectiveness of an entity in meeting its objectives. Management's role is to provide the leadership needed for an entity to realize that purpose. *Does this program accomplish what it is supposed to?* It is important that management remain focused on reaching intended objectives as well as day-to-day results.

Efficiency measures how well managers make use of available resources in achieving objectives. Because resources are always scarce, management is responsible for making the best use of the resources that are available. *Is resource use consistent with the department mission?*

Event Identification

Both internal and external events influence objectives and strategies. They may be isolated or part of a chain reaction or rippling effect. Events with a potential negative impact are considered risks while those with a potential positive impact are opportunities. Some of examples of events that affect organizations are:

- The organization's source of funding is being reduced or increased
- Employees' productivity is increasing or dropping
- Employees have different views of the organization's purpose
- The level of commitment of the person at the top of the organization is high or low

Risk Assessment

A risk assessment is a process to identify and analyze factors that may affect the achievement of a goal. In general, risk factors may include the control environment, size of the organization, complexity, change, and results of previous reviews/audits. It is important to remember that not all risks are equal. Some risks are more likely to occur while others will have a greater impact. For example, risks to safety or security of individuals, data or personal information could have significant consequences. Once identified, the assessment regarding the probability and significance of each risk is critical. The risk assessment design should be understandable, consider relevant risk factors and, to the extent possible, be objective.

Risk Response

Risk responses fall into four basic categories: (1) accept the risk and monitor it, (2) avoid the risk by eliminating it, (3) reduce the risk by instituting controls, or (4) share the risk by partnering or entering into a strategic alliance with another department or external entity.

Determining a risk response is an important decision. Because risk events by definition are uncertain, deciding whether to accept or avoid risk-related activity can have significant consequences for an organization. By choosing to reduce risk, an organization is committing to implement control activities which generally consume resources.

Controls

We divide controls into two main types – preventive and detective. A sound internal control plan will combine both preventive and detective controls to mitigate key risks. Preventive controls, as the term implies, work to prevent problems. However, since they may be time consuming and expensive, management should ensure that the benefits outweigh the cost. Examples of preventive controls include authorization lists, computer edits, segregation of duties, and prior supervisory approval.

Detective controls do not prevent fraud or errors. They will identify that a problem has occurred. On the other hand, detective controls are more efficient in that they do not slow business processes. They are less effective because they can only identify an incident after the fact, not stop it from happening. The existence of detective controls, however, can also serve to prevent irregularities. An individual tempted to use department funds inappropriately may be deterred by the knowledge that the bank account is regularly reconciled. Examples of detective controls include reconciliation, exception reports, and supervisory review.

Policies and Procedures

Controls are most frequently comprised of policies and procedures. After identifying and assessing risks, managers need to evaluate (and develop, when necessary) methods to minimize these risks. A policy establishes what should be done and serves as the basis for the procedures. Procedures describe specifically how the policy is to be implemented. It is important that an organization establish policies and procedures so that staff knows what is to be done and compliance can be properly evaluated.

Security

Department Head Signature Authorization

A department head is responsible for all activities conducted by the department. Because in most departments the department head cannot personally review and certify all business transactions, the department head is responsible for setting up the department's business operations with a series of checks and balances (internal controls) to balance risks and efficiencies. Department heads must directly authorize individuals within their chain of command to be their designee for approval of fiscal documents or other legal obligations on their behalf. There can be no sub-delegation by designees. See [State Finance Law and General Contract Requirements](http://www.mass.gov/Aosc/docs/policies_procedures/contracts/po_procon_state_finan law_gen_con_req.doc). (http://www.mass.gov/Aosc/docs/policies_procedures/contracts/po_procon_state_finan law_gen_con_req.doc)

Security of Records

Department management must ensure the security of records and sensitive information provided or available. The security of records and data in hard copy or electronic format involves system security, data security and physical security. Threats to security may come from within, as well as from the outside of an agency so consideration for each is needed.

System Security

Department management must determine each individual's HRCMS, MMARS and Warehouse security access by both business area and security level. Management can limit access to one or more specific business areas, such as Accounts Receivable, Payroll, or Fixed Assets. Within each business area, management must also select the appropriate security levels. In MMARS, the *Administrator* role is the most powerful since it allows the individual to validate and submit documents to final status. The *User* role is more restricted; it allows the processing of documents but excludes the ability to finalize documents.

Data Security

Data security is the means of protecting data, whether in hard media (paper, microfilm) or in computer and communications systems, against unauthorized disclosure, transfer, modifications or destruction whether accidental or intentional. Therefore, data security helps to ensure privacy. It also helps in protecting confidential data concerning clients, consumers and employees.

Data security consists of procedures that prevent unauthorized access to computer resources. Appropriate security procedures should not significantly hinder a person from performing their work. Security procedures should, however, protect data from unintentional acts, as well as intentional ones. Examples of data security include:

- Define carefully the level of system access an employee is given
- Select appropriate password safeguards
- A hard to guess password
- Periodic password changes
- Alphanumeric characters per password
- Password kept confidential
- Screen-saver passwords
- Assign each user a unique user ID
- Limit user access to system software

- Control access to specific applications and data files
- Limit access to what is required to perform a person's job function and to allow for appropriate segregation of duties
- Review security logs
- Limit concurrent logins
- Activate intruder detection and prevention mechanisms
- Implement adequate virus protection procedures

Access to enterprise systems should be reviewed quarterly, as well as when significant turnover occurs in sensitive positions or in realignment of duties.

Physical Security

Physical security is the protection of personnel, clients, records, and assets. This includes protection from fire, natural disasters, burglary, theft, vandalism, and terrorism. Security engineering involves three elements of physical security: (1) obstacles to frustrate trivial attackers and delay serious ones, such as locks and swipe card access; (2) detection devices such as alarms, security lighting, and security guards to make it likely that attacks will be noticed; and (3) security response to repel, catch or frustrate attackers when an attack is detected.

Segregation of Duties

Segregation of duties is a primary principle in any internal control plan in order to provide adequate checks and balances. The basic goal of segregation of duties is that no one person should have excessive control over one or more critical processes. It also defines authority and responsibility over activity and use of the Commonwealth's resources.

The fundamental premise of segregated duties is that an individual or small group of individuals should not be in a position to initiate, approve, undertake, and review the same action. These are called incompatible duties when performed by the same individual. The list below offers some examples of incompatible duties:

- Managing operations of an activity and record-keeping for the same activity
- Custody of assets and recording receipt of those assets
- Authorization of transactions and custody or disposal of the related assets or records
- Operating and programming computer system

Maintaining segregation of duties is especially challenging for units with small numbers of employees. Managers of such departments must consider this principle when designing and defining job duties; they must implement control procedures to assure segregation of duties exists. In an environment with limited numbers of personnel, management should develop alternate management procedures or reports to monitor financial activity or, if necessary, be involved in day-to-day activities of the unit, bureau or office.

Information

Management requires data to make effective decisions. Data alone is not enough, however; data provided must be the right information, in an understandable format, which is timely enough to be useful. Information systems produce reports, containing operational, financial, and compliance-related information that makes it

possible to run and control a department. This information should reveal the organization's progress toward meeting goals and objectives. Management also needs information that allows it to evaluate the efficiency of operations and to ensure that the organization follows applicable laws and regulations.

Questions to consider include the following:

- Does management regularly collect and review information that alerts it to both internal and external risks?
- Does the department get information that tells management whether it is achieving its objectives?

Communication

Communication is the exchange of useful information between and among people and organizations to support decisions and coordinate activities. Information should be communicated to management and other employees who need it in a form, and within a timeframe, that helps them to carry out their responsibilities.

Communication is multi-faceted – verbal, non-verbal and written. It is important to remember that effective verbal communication is two way, requiring that management welcome, and listen to, suggestions and feedback. Staff must be comfortable enough to share their awareness of problems with managers who can act on this information. Non-verbal messages, through gestures and facial expressions, are a major influence on creating a climate conducive to effective communication. Verbal communication should be in support of, not in place of, written documentation of policies and procedures. All written documentation, whether it is official policy/procedure, memo, or e-mail, must be distributed to anyone who requires the information in order to perform his or her responsibilities.

Communication is also multi-dimensional – from the top down, bottom up and across the organization. Effective communication informs all levels of the organization and must be ongoing. Communication systems can be formal or informal. Formal communication systems, from sophisticated computer technologies to staff meetings, provide input and feedback relative to an organization's activities, including the achievement of goals and objectives. Informal conversations with employees, contractors, vendors and regulators often provide some of the most critical information needed to identify risks and opportunities.

External communication can take a variety of forms, including annual reports, web sites, press releases, newsletters, and informational brochures. Other methods of communication include focus groups, presentations at conferences, and oral updates. Regardless of the methods used, maintaining open lines of communication with outside parties will enhance a department's internal control. For example:

Management should establish communication channels that:

- Provide timely information;
- Can be tailored to individual needs;
- Inform employees of their duties and responsibilities;
- Enable the reporting of sensitive matters;
- Enable employees to provide suggestions for improvement;
- Provide the information necessary for all employees to carry out their responsibilities;
- Convey top management's message that internal control responsibilities are important and should be taken seriously; and
- Convey and enable communication with external parties.

- Vendors, service providers, and consultants can provide significant input on the quality and design of agency products and services.
- Auditors, advocacy groups, and other outside reviewers can alert management to minor problems before they become major difficulties.
- Suppliers and contractors who are made aware of the agency's ethical standards can help deter or detect inappropriate purchasing or bidding practices.
- Complaints or inquiries can point out control problems, or the department's ability to supply accurate information to the media or concerned citizens.

Monitoring

Monitoring is the review of an organization's activities and transactions to assess the quality of performance over time and to determine whether internal controls are effective. Management should focus monitoring efforts on achievement of the organization's mission, goals and objectives. For example, management must consider whether internal controls are operating as intended and if they are appropriately modified when conditions change. The purpose of monitoring is to determine whether internal control is adequately designed, properly executed, and effective. Internal control is adequately designed and properly executed if all ERM components are present and functioning as designed.

In considering the extent to which the continued effectiveness of internal control is monitored, both ongoing monitoring activities and separate evaluations of the internal control structure should be considered. Ongoing monitoring occurs during normal operations and includes regular management and supervisory activities, comparisons, reconciliations, and other actions people take in performance of their duties. It includes ensuring that managers and supervisors know their responsibilities for internal control and the need to make control monitoring part of their regular operating processes. Separate evaluations are a way to take a fresh look at internal control by focusing directly on the control's effectiveness at a specific time. These evaluations may take the form of self-assessments as well as review of control design and direct testing, and may include the use of checklists.

For monitoring to be most effective, all employees need to understand the organization's mission, goals, objectives, risk levels and their own responsibilities. Everyone within an organization has some responsibility for monitoring. The position a person holds in the organization helps to determine the focus and extent of these responsibilities. Therefore, the monitoring performed by managers, supervisors and staff will not have the same focus. For example:

- Executive management should focus their monitoring activities on the major divisions within the organization. With this broad focus, they emphasize the organization's mission and goals.
- Managers assess how well internal controls function in multiple units within the organization.
- Supervisors monitor all activities within their respective units to ensure staff are performing their assigned responsibilities, internal control activities are functioning properly, and the unit is accomplishing its goals and objectives.

- Staffs monitor their own work to ensure it is being done properly. They should be trained by supervisors and management regarding internal controls and be encouraged to report any irregularities.
- Access to systems and sensitive data should be reviewed quarterly to ensure employees have needed access, but not more than what is needed to complete their responsibilities.

Authorization

Authorization is the power that management grants employees to carry out certain duties. It is a control activity designed to ensure that activities are authorized and executed only by persons acting within the scope of their authority. It is management that authorizes employees to perform certain activities and/or to execute certain transactions within limited parameters. Management should ensure that the conditions and terms of authorization are clearly documented and communicated.

Periodic Comparison/Reconciliation

The purpose of periodic comparison/reconciliation is to verify that the processing or recording of transactions is valid, properly authorized and recorded on a timely basis. Integral parts of the reconciliation process include identifying and investigating discrepancies from established standards, and taking corrective action when necessary.

Continuous Supervision

Qualified and continuous supervision must be provided to ensure that internal control objectives are achieved. Supervision is the ongoing oversight, management and guidance of an activity by designated employees to help ensure that the results of the activity achieve the established objectives. The duties of the supervisor in carrying out this responsibility should include:

- Clearly communicating the duties, responsibilities and accountability assigned to each staff member
- Systematically reviewing each employee's work to the extent necessary
- Approving work at critical points to ensure that work flows as intended

Recording Transactions

Departments must manage transactions and other significant events by their prompt recording, clear documentation and proper classification.

Access to Resources

Management is required to protect the organization's equipment, information, documents, and other resources that could be wrongfully used, damaged, or stolen. The department head is responsible for maintaining accountability for the custody and use of resources and shall assign qualified employees for that purpose. Management can protect resources by limiting access to authorized individuals. Access may be limited by various means such as locks, passwords, electronic firewalls, and encryption. Also, management must occasionally inventory the physical resources and the records to reduce the risk of unauthorized use or loss of resources and protect against wasteful and wrongful acts.

Documentation

Documentation involves preserving evidence to substantiate a decision, event, transaction, or system. All documentation should be complete, accurate, and recorded timely. It should have a clear purpose and be in a usable format that will add to the efficiency and effectiveness of the organization.

The department's internal controls, for example, should be clearly documented and readily available for examination. This documentation provides guidance for implementing controls and, along with department policies and procedures, sets forth the fundamental framework and the underlying methods and processes that all employees rely on to do their jobs. It provides specific direction to staff, helps form the basis for daily decisions, and can serve as a basis for training new personnel. Further, it is a necessary reference tool when management and auditors must attest to internal control effectiveness.

MMARS Audit Trail Reports

The Comptroller's Office has designated specific standard MMARS and LCM reports as audit trail reports. These reports provide a clear and auditable history of financial and labor distribution activities and are produced from data in the State's official accounting system. Audit trail reports are retained in Document Direct for the minimum retention period (generally three years) required for records conservation. Because under certain circumstances, departments may need to make these reports available for a longer period, departments may need to print or download the reports to retain them until the completion of ongoing audits or other requirements.

Evaluating the Internal Control Plan

Internal control is effected by people. It is not merely policy manuals and forms, but people at every level of the organization.

The management of each state agency is responsible for establishing and maintaining an effective internal control structure. To fulfill this responsibility, estimates and judgments by management are required to assess the expected benefits and related costs for internal control policies and procedures. The objectives of an internal control structure are to assist management in meeting objectives by providing reasonable assurance that assets are safeguarded against loss from unauthorized use or disposition. The internal control structure also ensures that financial transactions are executed in accordance with management's authorization and are recorded properly to permit the preparation of financial statements in accordance with generally accepted accounting principles (GAAP).

A well-designed internal control structure will reduce improper activity. The responsibility of designing and implementing internal controls is a continuous process. As conditions change, control procedures may become outdated and inadequate. Management must anticipate that certain procedures will become obsolete and modify the internal control structure in response to these changes. The questions below can assist the agency in evaluating internal controls regularly and in being responsive to changes in the internal control environment.

Evaluation Points

Consider the following questions as you evaluate your internal control plan:

1. Does the department have a written internal control plan? If so, when was it last updated?
2. Is the internal control plan a high-level summarization, on a department-wide basis, of the department's risks and of the controls used by the department to mitigate those risks?
3. Is the internal control plan supported by low-level detail such as departmental policies and procedures?
4. Was the department head and senior management instrumental in developing the plan?
5. Does the plan include the ERM components of:
 - a. Internal Environment
 - b. Objective Setting

- c. Event Identification
 - d. Risk Assessment
 - e. Risk Response
 - f. Control Activities
 - g. Information and Communication
 - h. Monitoring
6. Does the internal control plan include a department-wide risk assessment? Or, does the risk assessment include only fiscal? Are any business areas missing from the risk assessment?
 7. Do risks appear to match the stated mission, goals, and/or objectives?
 8. Does the risk assessment identify the most significant areas that could keep the department from attaining its mission, goals and objectives?
 9. Are the stated risks cross-referenced to internal controls?
 10. Do the policies, procedures and organizational structure (control activities) actively attempt to control the risks that were identified in the risk assessment?
 11. Does the internal control plan include information explaining how and when management monitors the objectives and activities contained in the plan?
 12. Does the internal control plan describe the method that should be used by staff to report internal control issues such as unresolved reconciling items and policy violations?
 13. Does the internal control plan indicate to whom in the department the internal control plan is distributed?
 14. Has the department trained employees in internal controls within the past year? Have employees attended the internal control training provided by the Office of the Comptroller?
 15. Has the department established unit(s) whose primary responsibility is internal audit, quality assurance, internal control or quality control? If yes, how many staff are assigned? What do they review? To whom do they report?
 16. Does the internal control plan describe the process to report unaccounted for variances, losses, shortages or theft of funds or property to the Office of the State Auditor?

Internal Control Plan Workbook

Internal control is a process. It is a means to an end, not an end in itself.

All operating departments in Massachusetts state government are required to develop and document departmental internal controls, which must be prioritized and summarized into a departmental internal control plan based on a risk assessment. Responsibility for the department internal control plan resides with the department's Internal Control Officer (ICO). The role of the ICO, as stated in Chapter 647 of the Acts of 1989, is described as follows: "...an official, equivalent in title or rank to an assistant or deputy to the department head, whose responsibility...shall be to ensure that the agency has written documentation of its internal accounting and administrative control system on file. Said official shall, annually, or more often as conditions warrant, evaluate the effectiveness of the agency's internal control system and establish and implement changes necessary to ensure the continued integrity of the system."

The Office of the Comptroller defines a department-wide risk assessment as the identification and analysis of the risks that could prevent the department from attaining its goals and objectives. This identification and analysis form the basis for determining the risk management strategy. A precondition to risk assessment is the establishment of the organization's mission and goals. A risk assessment is an integral part of an internal control plan.

The Office of the Comptroller defines an internal control plan as a high level department-wide summarization of the department's risks and the controls used to mitigate those risks. This high level summary must be supported by lower level detail, i.e. departmental policies and procedures.

Departments will find it helpful to use this workbook during their annual Internal Control Plan review or to further refine major programs, bureaus, institutions, or other department subdivisions.

Getting Started (Questions you must ask)

The questions below can be used as a starting point for internal control discussions and as concepts to consider while preparing or evaluating departmental internal controls.

Management
Does management emphasize by both word and action the importance of integrity and ethical values?
Does management place a high degree of importance on the work of external audits and other evaluations? Is management responsive to the results of the information?
Does top management set an example by following its own controls?

Objectives
How frequently are the mission and goals reviewed?
Are the objectives specific enough to clearly apply to this particular department?
Do objectives include measurement criteria?
Are the objectives clearly communicated to all employees?
Are the resources needed to meet the objectives available? If not, does management have plans to acquire resources?
Do program objectives flow from and link to the department-wide objectives?
Are all levels of staff included in establishing and achieving objectives relevant to their specific area of authority?

Risks
What potential circumstances could result in a failure to carry out the department's mission?
How frequently are these potential problems evaluated against changes in the mission or goals?
Do mechanisms exist to identify risks from external factors?
Are the controls appropriate to the risks? For example, are they too cumbersome or inadequate?

Policy and Procedure
Are documented policies and procedures in place for each major business and administrative area?
Are the current policies and procedures effective in reducing both the most harmful and the most likely risks?
How often are they reviewed?
How are policies and procedures, as well as any changes, communicated to staff?
How are policies and procedures tested? How often?
How often, and under what circumstances, do policies and procedures change?
How often is on-line access to departmental and statewide systems reviewed by senior management?

Your Workbook (Linking internal controls to risks)

What is your mission statement?

Mission Statement

What are your long range goals that support your mission statement?

1. Goal #1
2. Goal #2
3. Goal #3

What are the short term objectives that support each of your long range goals?

1. Goal #1
 - a. Objective #1 for Goal #1
 - b. Objective #2 for Goal #1
 - c. Objective #3 for Goal #1
 - d. Objective #4 for Goal #1
2. Goal #2
 - a. Objective #1 for Goal #2
 - b. Objective #2 for Goal #2

What are the risks associated with each objective?

1. Goal #1
 - a. Objective #1 for Goal #1
 - i. Risk #1 for Objective #1 for Goal #1
 - ii. Risk #2 for Objective #1 for Goal #1
 - b. Objective #2 for Goal #1
 - i. Risk #1 for Objective #2 for Goal #1
 - ii. Risk #2 for Objective #2 for Goal #1

What are the internal controls to mitigate the risks?

2. Goal #1
 - a. Objective #1 for Goal #1
 - i. Risk #1 for Objective #1 for Goal #1
 - a. Internal Control #1 for Risk #1 of Objective #1 for Goal #1
 - b. Internal Control #2 for Risk #1 of Objective #1 for Goal #1
 - ii. Risk #2 for Objective #1 for Goal #1
 - a. Internal Control #1 for Risk #2 of Objective #1 for Goal #1
 - b. Internal Control #2 for Risk #2 of Objective #1 for Goal #1
 - b. Objective #2 for Goal #1
 - i. Risk #1 for Objective #2 for Goal #1
 - a. Internal Control #1 for Risk #1 of Objective #2 for Goal #1
 - b. Internal Control #2 for Risk #1 of Objective #2 for Goal #1
 - ii. Risk #2 for Objective #2 for Goal #1
 - a. Internal Control #1 for Risk #2 of Objective #2 for Goal #1
 - b. Internal Control #2 for Risk #2 of Objective #2 for Goal #1

Annual Reporting

Internal control can be expected to provide only reasonable assurance, not absolute assurance, to an entity's management and board.

The Massachusetts Statewide Single Audit (SSA) is an annual comprehensive review, by fiscal year, of the Commonwealth's strengths and weaknesses in the areas of internal controls and compliance with federal grant regulations. The Single Audit Act, as amended in 1996, and Office of Management and Budget (OMB) Circular A-133 require single audits to provide the federal government with reasonable assurance on the accuracy of financial statements and on major programs' compliance with federal laws and regulations. Other audits must, by law, build on the work of the single audit rather than duplicate it. As directed by the Governor and Legislature, the Office of the Comptroller procures audit services for, and directs the operation of, the SSA. An independent accounting firm, selected through a competitive bidding process, conducts this audit. The Office of the State Auditor provides resources and audit work in support of the Single Audit. The audit process is directed by a management team comprised of staff from the Office of the Comptroller, the Office of the State Auditor, and the independent accounting firm. As part of the audit, Commonwealth management is required to disclose to the independent auditor any and all audits, reviews or investigations by an outside regulatory entity, whether federal or state, so that the auditors may evaluate the relevance of that investigation to the audit. The department must contact the Comptroller's Office if it has been notified of a federal audit, other regulatory review or investigation, or program review so we can coordinate those activities with the single audit. By coordinating with the federal auditors, the same issues will not need to be re-reviewed.

At the beginning of each SSA, auditors perform a preliminary evaluation of the Commonwealth's internal controls. They then review the internal controls of some departments in more depth. The auditors use departments' internal control plans and Internal Control Questionnaire responses, along with other procedures, to render an opinion on the internal controls of the Commonwealth as a whole.

Internal Control Questionnaire

The Internal Control Questionnaire, commonly known as the ICQ, is one component of the SSA. Each spring, at the beginning of the audit cycle, the Office of the Comptroller distributes the questionnaire to all departments. This web-based survey is designed to provide insight into departmental internal control procedures. Because of its length, questions are divided by topic into multiple sections; however, because not all questions are applicable to all departments, most departments are able to skip one or more of these sections.

The Comptroller recommends that the internal control officer, the single audit liaison, and the chief fiscal officer work closely with senior management in responding to these questions. In most departments, several individuals will need to be involved. Auditors review the ICQ responses as part of the annual planning process and may contact department staff to follow up on some of the questions.

Departments Using Centralized Business Units

Because of the restructuring of state government over the past few years, many departments use secretariat level centralized business units (shared service centers) to perform functions including, but not limited to, human resources, payroll, accounting, and procurement processing. If your department utilizes a shared service center to process centralized business functions, answer the questions as you would if your department used a contractor to perform them. In the comments section, briefly describe the arrangement.

Representations

The last piece of the Questionnaire is the *representations* section. In this section, the department head, the chief fiscal officer, and the internal control officer must read and approve the statements, confirming that the information entered into the questionnaire is accurate. ([The responsibilities of these key personnel are defined in the Comptroller's Key Appointments policy](http://www.mass.gov/Aosc/docs/Forms/Security/Dept%20Key%20State%20Finance%20Law.doc) [http://www.mass.gov/Aosc/docs/Forms/Security/Dept Key State Finance Law.doc].) Enter names and official titles in the appropriate section of the form. Staff should plan to provide a copy to any auditors who come to your agency as part of the Statewide Single Audit.

Conclusion

Each of us plays a vital role in creating an environment that is accountable to the public while being responsive to the needs and direction of senior management. Internal controls are a critical element of this environment.

APPENDIX 1

Regulations and Guidance

Chapter 647 of the Acts of 1989

In accordance with [M.G.L. c. 7A, s. 9A](#) and [Chapter 647 of the Acts of 1989](#), *An Act Relative to Improving the Internal Controls within State Agencies*, the Office of the Comptroller (CTR) is directed to work with the Office of the State Auditor (OSA) to publish minimum standards for internal control systems at state departments for administrative and financial operations. The Internal Control Laws require that departmental internal control structure be developed in accordance with the internal control guideline established by the CTR.

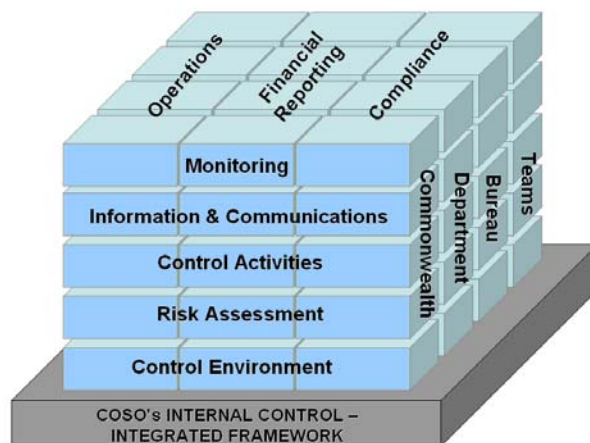
Each department is required to designate a high-ranking official, in addition to his or her regular duties, the responsibility of maintaining the written documentation of the internal control structure and evaluate the effectiveness of the structure annually, or more often as conditions warrant, to ensure the continued integrity of the structure. This official also has the responsibility to take timely corrective action on audit results and implement the audit recommendations.

The law also requires that all unaccounted for variances, losses, shortages or thefts of funds or property, are immediately reported to the OSA. The OSA has the responsibility to determine the internal control weaknesses that contributed to the condition, identify the internal control policies and procedures that need modifications, identify the amount of funds involved, make recommendations that address the correction of the condition found, and report the matter to appropriate management and law enforcement officials.

The Internal Control Laws are an integral part of State Government to provide reasonable assurance that departments' financial and programmatic operations are effective, efficient, and reliable and are in compliance with applicable laws, rules and regulations.

COSO

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) was created in 1987 to identify factors associated with fraudulent financial reporting and to make recommendations to reduce fraud. COSO then retained Coopers & Lybrand, a major CPA firm, to study the issues and author a report regarding an integrated framework of internal control. The Coopers & Lybrand authored report, issued in 1992 and re-published with minor amendments in 1994, was entitled *Internal Control - Integrated Framework*. This report presented a common definition of internal control and provided a framework against which internal control systems can be assessed and improved.



As stated on its web site, “COSO is a voluntary private sector organization dedicated to improving the quality of financial reporting through business ethics, effective internal controls, and corporate governance.” COSO is jointly sponsored by the American Accounting Association, the American Institute of Certified Public Accountants, Financial Executives International, the Institute of Internal Auditors, and the Institute of Management Accountants.

Internal Control – Integrated Framework

COSO defines internal control as “a process, effected by an entity’s board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories: effectiveness and efficiency of operations, reliability of financial reporting, compliance with applicable laws and regulations.”

In other words, internal controls are tools that help managers be effective and efficient while avoiding serious problems such as overspending, operational failures, and violations of law.

Internal control has been further defined as consisting of five interrelated components:

1. The **control environment** sets the tone of the organization and influences the effectiveness of internal controls.
2. A **risk assessment** is the process used to identify, analyze, and manage the potential risks that could hinder or prevent the achievement of goals and objectives.
3. The **control activities** established to minimize the identified risks include structure, policies, and procedures.
4. **Information and communication** is the means by which risks, policies, and procedures are shared with members of the organization.
5. By **monitoring** the effectiveness of internal controls, an organization ensures that their controls reflect the current environment.

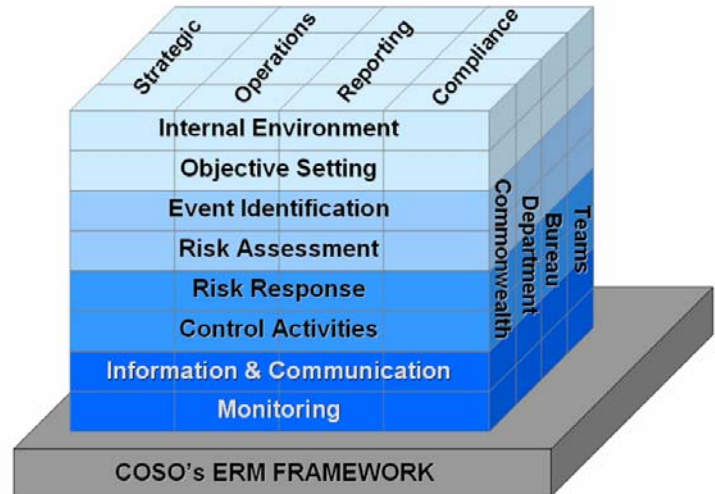
Because internal controls are a means to an end, they must help, rather than prevent or delay, an organization in reaching its objectives. Before designing and implementing internal controls, managers should consider the following four basic principles:

- Internal controls must benefit, rather than hinder, the organization.
- Internal controls must make sense within each organization’s unique operating environment.
- Internal controls are not stand-alone practices. They are woven into the day-to-day responsibilities of managers and their staff.
- Internal controls must be cost effective.

Enterprise Risk Management – Integrated Framework

In September 2004, COSO issued its framework for enterprise-wide risk management, *Enterprise Risk Management – Integrated Framework* also known as COSO II. Enterprise Risk Management (ERM) is a broader framework that incorporates key concepts set out in COSO’s earlier *Internal Control – Integrated Framework*. ERM augments the original framework because they are based on the same conceptual foundation. ERM is defined as “...a process, effected by an entity’s board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage the risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity

objectives.” The ERM framework requires an entity to take a portfolio view of risk from two perspectives: business unit level and entity level. It expands and elaborates on the risk assessment and internal environment components of the Internal Control – Integrated Framework. For example, it breaks out internal environment into two components (internal environment and objective setting) and risk assessment into three components (event identification, risk assessment and risk response).



The eight interrelated components of ERM:

1. The **internal environment** is the tone of an organization which, among other things, determines an organization’s “risk culture” and provides the basis for its internal controls.
2. **Objective setting** is a critical process that supports an organization’s mission.
3. **Event identification** identifies internal and external events that impact an organization achieving its objectives. Events that may have a negative impact represent risks while those that may have a positive impact represent opportunities.
4. The **risk assessment** allows an organization to understand the extent to which potential events may impact objectives. Risks should be assessed from both the likelihood of happening and the impact if it happens.
5. The **risk response** evaluates options to an identified risk and determines the course of action. Options available are (a) accept the risk and monitor it, (b) avoid the risk by eliminating it, (c) reduce the risk by implementing controls, and (e) share the risk with another entity.
6. An organization’s **control activities** include policies and procedures, directives, etc. They occur throughout the organization at all levels and functions.
7. **Information and communication** is the identification and dissemination of pertinent information in a form and timeframe that enables people to carry out their responsibilities. Communication occurs in all directions – flowing down, across and up the organization.
8. **Monitoring** the effectiveness of components includes ongoing activities and/or separate evaluations and making modifications as necessary.

Yellow Book

The Comptroller General of the United States issues *Government Auditing Standards* (known as the Yellow Book, January 2007 Revision), through the U.S. Government Accountability Office (GAO). These standards, also referred to as generally accepted government auditing standards (GAGAS),

The revised “Yellow Book” issued by David M. Walker, Comptroller General of the United States and head of the U.S. Government Accountability Office, emphasizes the critical role of the government audits in achieving credibility and accountability in government, with an increased focus on the ethical principles underlying the work of those who audit government programs and activities.

explain the rules that auditors must follow during audits of governmental entities, programs, activities, and functions. Audit organizations must also use *Government Auditing Standards* during reviews of governmental assistance that is administered by contractors and nonprofit organizations, when required by statute or other mandates, or when auditors hold themselves out as following government auditing standards. The Yellow Book establishes requirements for auditors' professional qualifications, the quality of audit effort, and the characteristics of professional and meaningful audit reports. It includes requirements and guidance for the following types of reviews: financial audits, attestation engagements, and performance audits.

Sarbanes-Oxley (SOX)

The Sarbanes-Oxley Act of 2002, also known as the Public Company Accounting Reform and Investor Protection Act of 2002 is a federal law passed in response to several major corporate and accounting scandals (Enron, Tyco, and WorldCom). The law is comprehensive and strengthens standards for all U.S. public company boards, management, and public accounting firms. It instituted drastic changes for the accounting profession, especially in the area of auditor independence.

Auditing has become more of a regulated industry post-SOX. Organizations have greater financial reporting and control responsibilities and auditors are expected to hold their clients to a higher standard of accountability for financial reporting and compliance controls as well as financial reporting transparency. SOX requires management to establish and maintain adequate internal controls and procedures for financial reporting. It also emphasizes that management is responsible for internal controls.

The Director of the U.S. Government Accountability Office (GAO) states that “where appropriate, auditor opinions on internal control are critical for monitoring an organization’s internal control and accountability”. While most provisions of SOX apply only to public companies and their auditors, many oversight agencies have pushed to use SOX to increase the accountability of public sector groups, mostly non-profit organizations. Recently, there has been an effort to use the reforms included in SOX to increase the accountability and mitigate the risks of state and local governments.

OMB Circular A-123

In December 2004, the Office of Management and Budget (OMB) reissued Circular number A-123 to define the management responsibilities for internal financial controls in federal agencies. This Circular provides guidance to federal managers on improving the accountability and effectiveness of federal programs and operations by establishing, assessing, correcting, and reporting on management controls. Circular A-123 is a re-examination of the existing internal control requirements for federal agencies and was initiated in light of the new internal control requirements for publicly-traded companies contained in the Sarbanes-Oxley Act of 2002. Under A-123, agencies and individual federal managers are required to take systematic and proactive measures to:

1. Develop and implement appropriate, cost-effective management controls for results-oriented management,
2. Assess the adequacy of management controls in federal programs and operations,
3. Identify needed improvements,
4. Take corresponding corrective action, and
5. Report annually on management controls.

OMB Circular A-133

In June 1996, the Office of Management and Budget (OMB) issued a revised Circular A-133, Audits of States, Local Governments, and Non-Profit Organizations, to provide administrative guidance for implementing the single audit requirements. A single audit is an organization-wide audit that includes both the entity's financial statements as well as its federal awards. Effective January 2004, A-133 audit guidelines require entities that expend \$500,000 or more a year in federal awards to have a single or program-specific audit conducted. Under A-133, those governments or organizations that expend \$500,000 or more in federal awards during the fiscal year must do the following:

1. Maintain internal control for federal programs,
2. Comply with the laws, regulations, and the provisions of contracts or grant agreements,
3. Prepare appropriate financial statements, including the schedule of expenditures of federal awards,
4. Ensure that the required single audits are properly performed and submitted when due, and
5. Follow up and take corrective actions on audit findings.

SAS No. 112

In May 2006, the AICPA issued Statement on Auditing Standards (SAS) No. 112, Communicating Internal Control Related Matters Identified in an Audit. It is effective for audits of financial statements for periods ending on or after December 15, 2006. SAS No. 112 has two unconditional requirements: (1) the auditor must evaluate identified control deficiencies and determine whether those deficiencies, individually or in combination, are significant deficiencies or material weaknesses; and (2) the auditor must communicate, in writing, significant deficiencies and material weaknesses to management and those charged with governance. It is likely that more audit findings will be reportable because SAS No. 112 clarifies the significance of a control deficiency is dependent on the potential for misstatement, not whether the misstatement actually occurred.

Audit Committee

Within the public sector, an audit committee is an extension of the governing body. Committees are formed to fulfill the governing body's responsibilities, not expand them. Officials are able to increase their oversight of specific issues by assigning various matters to committees.

In this light, the audit committee is an integral element of public accountability and governance. It plays a key role for the governing body in carrying out its legal and fiduciary responsibilities, especially with respect to the integrity of the government's financial information, system of internal control, and legal and ethical conduct of management and employees.

The roles of the audit committee may vary from entity to entity depending on the complexity and size, as well as the requirement of the governing body. However, the one common responsibility for all audit committees, among all their potential roles, is risk management oversight.

An audit committee has three fundamental goals. First, it must satisfy itself that management is maintaining a comprehensive framework of internal control. Second, the audit committee must ensure that management's financial reporting practices are assessed objectively. Third, the committee needs to determine to its own satisfaction that the financial statements are properly audited and that any problems disclosed in the course of the audit are satisfactorily resolved.

- *Audit Committees* by Stephen J. Gauthier

Every organization faces a variety of potential risks, such as:

- Loss of key staff
- Loss of funding or reduction of revenue sources
- Regulatory non-compliance
- Conflicts of interest
- Fraudulent activities resulting from weaknesses in internal controls

Internal Audit

As defined by the Institute of Internal Auditors, “Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization’s operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes.”

Management is responsible for establishing and maintaining an adequate system of internal controls. An internal audit office is charged by management with “... assessing the effectiveness of the design and execution of the system of internal controls and risk management processes.”

Internal auditors continuously evaluate risk exposures in relation to:

- Effectiveness and efficiency of operations
- Reliability and integrity of financial and operational information
- Safeguarding of assets
- Compliance with laws, regulations and contracts
- Accomplishment of established operational goals and objectives

Internal auditors are responsible for making recommendations for improvement in internal controls to top management and, if applicable, a governing board of directors. To maintain independence, and to perform in an objective capacity, internal auditors should not engage in any operational or programmatic responsibilities.

APPENDIX 2

Works Cited

- Auditing – An Integrated Approach by Alvin A. Arens, Randal J. Elder and Mark S. Beasley.
- Audit Committees by Stephen J. Gauthier, Government Finance Officers Association, Chicago, IL 2006.
- Circular No. A-123. Office of Management and Budget.
<http://www.whitehouse.gov/omb/circulars/a123/a123.html>
- Circular No. A-133. Office of Management and Budget.
<http://www.whitehouse.gov/omb/circulars/a133/a133.html>
- COSO. The Committee of Sponsoring Organizations of the Treadway Commission.
<http://www.coso.org>
- Government Auditing Standards (The Yellow Book). <http://www.gao.gov/SOX>
- Encyclopedia Mythica, 2004, 13 May 2004 <http://www.pantheon.org>
- Enterprise Risk Management – Integrated Framework Executive Summary by the Committee of Sponsoring Organizations of the Treadway Commission. September 2004.
- Evaluating Internal Controls – A Local Government Manager’s Guide by Stephen J. Gauthier, Government Finance Officers Association, Chicago, IL 1996.
- Improving Governance and Internal Controls over Financial Reporting in the Public Sector by KPMG, LLP 2005.
- Public Sector Audit Committees, Resource Guide by Deloitte & Touche LLP May 2003.
- SAS No. 112. American Institute of Certified Public Accountant (AICPA).
<http://www.aicpa.org/default.aspx>
- Single Audit Information Service. Thompson Publishing Group State of Connecticut Accountability Directive Number 1. [http:// www.osc.state.ct.us/manuals/AcctDirect/manual.htm](http://www.osc.state.ct.us/manuals/AcctDirect/manual.htm)